

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

|  |   |                      |
|--|---|----------------------|
| CHARLENE FIGUEROA and JERMAINE BURTON,                       | ) |                      |
| individually and on behalf of all others similarly situated, | ) |                      |
|  | ) | 19 C 1306            |
| Plaintiffs,  | ) |                      |
|  | ) | Judge Gary Feinerman |
| vs.  | ) |                      |
|  | ) |                      |
| KRONOS INCORPORATED,   | ) |                      |
|  | ) |                      |
| Defendant.   | ) |                      |

**MEMORANDUM OPINION AND ORDER**

Charlene Figueroa and Jermaine Burton brought this putative class action in the Circuit Court of Cook County, Illinois, against Kronos, Inc., alleging violations of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1 *et seq.* Doc. 1-1. Kronos timely removed the suit under 28 U.S.C. § 1453(b), premising jurisdiction on the Class Action Fairness Act, 28 U.S.C. § 1332(d). Doc. 1. Kronos moves under Civil Rule 12(b)(6) to dismiss the complaint, Doc. 29, and, in the alternative, under Civil Rule 23(c)(1)(A) to strike its class allegations, Doc. 32. Both motions are denied, though the court orders supplemental briefing regarding Plaintiffs’ standing to pursue their claim under Section 15(a) of BIPA, 740 ILCS 14/15(a).

**Background**

In resolving a Rule 12(b)(6) motion, the court assumes the truth of the operative complaint’s well-pleaded factual allegations, though not its legal conclusions. *See Zahn v. N. Am. Power & Gas, LLC*, 815 F.3d 1082, 1087 (7th Cir. 2016). The court must also consider “documents attached to the complaint, documents that are critical to the complaint and referred to in it, and information that is subject to proper judicial notice,” along with additional facts set forth in Plaintiffs’ brief opposing dismissal, so long as those additional facts “are consistent with

the pleadings.” *Phillips v. Prudential Ins. Co. of Am.*, 714 F.3d 1017, 1020 (7th Cir. 2013) (internal quotation marks omitted). The facts are set forth as favorably to Plaintiffs as those materials allow. *See Pierce v. Zoetis, Inc.*, 818 F.3d 274, 277 (7th Cir. 2016). In setting forth the facts at the pleading stage, the court does not vouch for their accuracy. *See Goldberg v. United States*, 881 F.3d 529, 531 (7th Cir. 2018).

Kronos is a provider of human resource management software and services. Doc. 1-1 at ¶ 1. As part of its business, Kronos provides timekeeping systems to thousands of employers in Illinois. *Ibid.* Those systems include biometric-based time clocks, which require employees to use their biometric information to punch in and out of work. *Id.* at ¶ 2.

When beginning work for an employer that uses a Kronos biometric timekeeping device, an employee must have her fingerprint or palm print scanned to enroll in the Kronos database. *Id.* at ¶ 25. Kronos does not inform those employees that it is collecting, storing, or using their biometric data. *Id.* at ¶¶ 26-27. Nor does Kronos inform them of the purposes for collecting their data or to whom the data is or will be disclosed. *Ibid.* Kronos does not maintain retention schedules or guidelines for permanently destroying the data. *Id.* at ¶¶ 28, 32. Kronos has not destroyed biometric data when the initial purpose for obtaining it has been satisfied or within three years of an employee’s last interaction with her employer. *Id.* at ¶ 32. Employees are not told whether and to whom Kronos discloses their data or what would happen to the data in the event of a Kronos merger or bankruptcy. *Id.* at ¶ 33.

Figueroa worked as an hourly employee at Tony’s Finer Food Enterprises Inc. from March 2017 through September 2018. *Id.* at ¶ 35. Burton worked for BWAY from January 2017 through April 2017. *Id.* at ¶ 49. Both were required, as a condition of their employment, to scan their fingerprints using a Kronos device to track their time. *Id.* at ¶¶ 35, 49. Both scanned

their fingerprints when clocking in or out of work, *id.* at ¶¶ 37, 51, and Figueroa did so when clocking in and out for lunch, *id.* at ¶ 38.

Kronos stored Plaintiffs' fingerprint data in its database or databases. *Id.* at ¶¶ 36, 50. At no point were Plaintiffs informed of the purposes or length of time for which Kronos was collecting, storing, using, or disseminating their data. *Id.* at ¶¶ 39, 52, 80. Nor were Plaintiffs informed of any biometric data retention policy developed by Kronos or whether it would ever permanently delete their data. *Id.* at ¶¶ 40, 53, 81. That is because Kronos lacked such a policy when Plaintiffs were hired, *id.* at ¶¶ 28, 81, which means that it failed to adhere to or publish such a policy at that time, *id.* at ¶¶ 73-74—though “years later” it implemented and published a policy, “long after being sued in other BIPA actions,” Doc. 50 at 14-15.

At no point did Plaintiffs receive or sign a release allowing Kronos to collect, store, use, or disseminate their biometric data. Doc. 1-1 at ¶¶ 41, 54. Nonetheless, Kronos disseminated their data to other firms, including firms hosting the data in data centers. *Id.* at ¶¶ 45, 79. Plaintiffs would not have provided their data to Kronos had they known it would retain the data for an indefinite time period without their consent. *Id.* at ¶¶ 43, 56.

### **Discussion**

BIPA “regulat[es] the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” 740 ILCS 14/5(g). “Biometric identifier” is defined to include a “fingerprint.” 740 ILCS 14/10. A biometric identifier is particularly sensitive because, unlike a social security number, it cannot be “changed,” which means that “once [it is] compromised, the individual has no recourse[ and] is at heightened risk for identity theft.” 740 ILCS 14/5(c). Recognizing this concern, Illinois adopted BIPA to protect the

privacy of biometric data. *See Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1206-07 (Ill. 2019).

The complaint alleges violations of Sections 15(a), 15(b), and 15(d) of BIPA. Section 15(a) requires private entities that possess biometric data to develop and publish a written policy that includes a retention schedule and destruction guidelines. 740 ILCS 14/15(a). Section 15(b) provides that, in order to collect a person's biometric data, a private entity must first (1) inform the person that the data is being collected or stored; (2) inform the person of the "specific purpose and length of term" for which the data is being collected, stored, and used; and (3) receive a written release from the person. 740 ILCS 14/15(b). Section 15(d) provides that, in order to disclose or otherwise disseminate a person's biometric data, a private entity must, absent exceptions inapplicable here, obtain the person's consent. 740 ILCS 14/15(d). BIPA allows a private right of action by "[a]ny person aggrieved by a violation." 740 ILCS 14/20.

## **I. Plaintiffs' Standing**

Where, as here, a case is removed from state court, "[i]f at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded." 28 U.S.C. § 1447(c). Although no party raises a jurisdictional issue, the court has an independent responsibility to ensure that it has subject matter jurisdiction. *See Carroll v. Stryker Corp.*, 658 F.3d 675, 680 (7th Cir 2011). The issue is close enough to warrant discussion.

A federal court has subject matter jurisdiction only if the plaintiff has Article III standing. *See MAO-MSO Recovery II, LLC v. State Farm Mut. Auto. Ins. Co.*, 935 F.3d 573, 581 (7th Cir. 2019). "[T]he irreducible constitutional minimum of standing consists of three elements. The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citation and internal quotation marks

omitted). “To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” *Id.* at 1548 (internal quotation marks omitted).

To be concrete, a plaintiff’s injury “must be de facto; that is, it must actually exist,” meaning that it must be “real” and not “abstract.” *Id.* at 1548 (internal quotation marks omitted). Both “tangible” and “intangible” injuries, even those that are “difficult to prove or measure,” can be concrete. *Id.* at 1549. Concreteness requires at least some “appreciable risk of harm” to the plaintiff. *Meyers v. Nicolet Rest. of De Pere, LLC*, 843 F.3d 724, 727 (7th Cir. 2016); *see also Spokeo*, 136 S. Ct. at 1550 (holding that an injury is not concrete where the defendant’s conduct does not “cause harm or present any material risk of harm”); *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 911 (7th Cir. 2017) (holding that the plaintiff lacked standing where he identified no “plausible (even if attenuated) risk of harm to himself”).

As the Seventh Circuit explained in *Robertson v. Allied Solutions, LLC*, 902 F.3d 690 (7th Cir. 2018), a defendant’s “withholding information when a statute requires its publication” inflicts an “informational injury.” 902 F.3d at 694. “An informational injury is concrete” for standing purposes “if the plaintiff establishes that concealing information impaired her ability to use it for a substantive purpose that the statute envisioned.” *Ibid.* While a failure to disclose “substantive information” “harm[s] the concrete interest that the [relevant] statute protect[s],” whether the failure to disclose information that merely “give[s] notice of” the plaintiff’s “statutory rights” does so depends on the circumstances. *Casillas v. Madison Ave. Assocs., Inc.*, 926 F.3d 329, 334-35 (7th Cir. 2019). Specifically, the failure to disclose information concerning the plaintiff’s statutory rights inflicts a concrete injury where the defendant fails entirely to make the disclosure, but not where the defendant only makes an incomplete or

otherwise technically deficient disclosure. *See Lavallee v. Med-1 Sols., LLC*, 932 F.3d 1049, 1053 (7th Cir. 2019) (holding that the plaintiff alleged an injury-in-fact where she “never received *any* of the disclosures required by” the statute in question, and distinguishing *Casillas* in part on the ground that the plaintiff there merely “received an *incomplete* validation notice”).

Earlier this year, the Seventh Circuit held in *Crabtree v. Experian Information Solutions, Inc.*, 948 F.3d 872 (7th Cir. 2020), that where the defendant’s violation of a statutory duty to disclose leads “to the deprivation of an opportunity [for the plaintiff], even if futile as a practical matter, [that] can be enough to establish a concrete injury.” *Id.* at 878. In *Robertson*, for instance, the employer violated the Fair Credit Reporting Act by “fail[ing] to provide the plaintiff with a copy of her background report before rescinding her employment offer.” *Ibid.* That injury, *Crabtree* explained, “was concrete enough [to establish standing] because the plaintiff ... lost the benefit of ‘her interest in responding’ to information in her background report, even if the information was accurate and she would have been unable to convince the prospective employer to honor the original offer.” *Ibid.* (quoting *Robertson*, 902 F.3d at 697).

Under these principles, Plaintiffs have standing to pursue their claims under Sections 15(b) and 15(d). The complaint alleges that Kronos obtained Plaintiffs’ biometric data without informing them it was doing so or obtaining their consent, in violation of Section 15(b), Doc. 1-1 at ¶¶ 25-27 (“Kronos fails to inform ... employees that Kronos is collecting, storing or using their sensitive biometric data ... or to whom the data is disclosed ...”), and that Kronos disclosed or otherwise disseminated their data to outside data hosts without informing Plaintiffs or obtaining their consent, in violation of Section 15(d), *id.* at ¶¶ 79-80 (“Defendant systematically disclosed Plaintiffs’ biometric identifiers and biometric information to other currently unknown third parties, which hosted the biometric data in their data centers.”). With

both claims, Plaintiffs were denied an opportunity to withhold their consent to the collection or dissemination of their data. That was no mere technicality, for without being informed that Kronos or outside data hosts would obtain their data, Plaintiffs were denied entirely an opportunity to object, in any fashion, to the way their data was handled. Doc. 1-1 at ¶¶ 43, 56 (alleging that Plaintiffs “would not have provided [their] biometric data to Defendant if [they] had known that [Kronos] would retain such information for an indefinite period of time without [their] consent”). Under *Crabtree*, the denial of that opportunity is sufficiently concrete to confer standing.

This feature of Plaintiffs’ claims under Sections 15(b) and 15(d) serves to distinguish recent BIPA decisions holding that the plaintiffs in those cases lacked standing. In all but one of those cases, the plaintiffs knowingly provided biometric data to their employers but did *not* allege that the employers redisclosed that data, which meant that they had ample opportunity to object to the employers’ collection (and potential dissemination) of the data even if their consent to the collection was not solicited in the specific manner required by BIPA. *See Hunter v. Automated Health Sys., Inc.*, 2020 WL 833180, at \*1-2 (N.D. Ill. Feb. 20, 2020) (holding that the plaintiff lacked standing where she “fail[ed] to allege that defendant collected her biometric data without her knowledge or created a risk that [the] data would fall into the hands of an unauthorized third party”); *Bryant v. Compass Grp. USA, Inc.*, \_\_ F. Supp. 3d \_\_, 2020 WL 433868, at \*2-3 (N.D. Ill. Jan. 28, 2020) (holding that the plaintiff lacked standing because the defendant “did nothing with Plaintiff’s data about which she was not aware” and the plaintiff did “not allege that Defendant shared her biometric information with third parties or created an immediate risk that such data would fall into the hands of third parties”); *Colon v. Dynacast, LLC*, 2019 WL 5536834, at \*2-4 (N.D. Ill. Oct. 17, 2019) (“Because Plaintiff knew that her data

was being collected, Defendant's failure to go through each procedural formality outlined in BIPA did not ... [constitute an] injury in fact. Similarly, because Plaintiff has not alleged that her data was given to third-parties, her right to privacy in her biometric data was not compromised.") (citation omitted). Although one decision found no standing where the complaint alleged that the plaintiff's employer disclosed biometric data to an outside payroll vendor, the court acknowledged that the "issue of disclosure to non-parties presents a close legal question" and made its ruling before the Seventh Circuit further clarified the law in *Crabtree*. *McGinnis v. U.S. Cold Storage, Inc.*, 2019 WL 7049921, at \*2-4 (N.D. Ill. Dec. 23, 2019).

Standing for Plaintiffs' Section 15(a) claim turns on whether Kronos's failure to develop and publish a retention schedule and guidelines for the destruction of biometric data inflicted the type of informational injury that qualifies as concrete. An entity's publication of a Section 15(a) disclosure provides substantive information about how a person's biometric data is handled, as opposed to information that merely describes the person's statutory rights. Had Kronos timely published its retention schedule and guidelines, Plaintiffs might have become aware sooner that Kronos was collecting their biometric data and sending it to outside data hosts, and thus could have taken quicker action to ensure that their data was being properly handled. Doc. 1-1 at ¶¶ 28, 32, 80, 83 (alleging that Kronos "collected, stored, and used employees' biometric data for years without" providing "employees with a written, publicly-available policy identifying its retention schedule and guidelines for permanently destroying employees' biometric data"). That said, the complaint acknowledges that due to Kronos's alleged violations of Sections 15(b) and (d), "most employees don't know they are interacting with Kronos when they have their biometrics scanned by their employer's Kronos devices, let alone providing it their biometric data," and therefore would "have no reason to affirmatively seek out Kronos' website and search



for its biometric data policies.” *Id.* at ¶ 28. If Plaintiffs would never have sought out a biometric data policy published by Kronos, it is unclear whether they suffered any concrete injury due to Kronos’s failure to develop and publish such a policy.

Given these considerations, the court cannot with the requisite level of confidence ascertain whether Plaintiffs have standing to pursue their Section 15(a) claim. Accordingly, the court directs the parties to submit supplemental briefing addressing whether—in light of the principles discussed above—Plaintiffs have standing to pursue that claim. If the court ultimately concludes that Plaintiffs have standing, it then will rule on Kronos’s motion to dismiss the Section 15(a) claim, relying on the parties’ existing Rule 12(b)(6) briefing.

## **II. Kronos’s Motion to Dismiss**

### **A. Section 15(b) Claim**

Section 15(b) of BIPA provides:

No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, unless it first:

(1) informs the subject ... in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject ... in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information ... .

740 ILCS 14/15(b). Thus, as a “private entity” that “obtain[ed]” Plaintiffs’ biometric data, Kronos “first” had to “inform[]” them that it was collecting or obtaining their data and for what “purpose and length of term,” and receive from them a “written release.” *Ibid.* The complaint alleges that when Plaintiffs enrolled in and used their employers’ timekeeping systems, Kronos obtained their biometric data without first informing them or obtaining from them a written

release. Doc. 1-1 at ¶¶ 25- 27, 35-38, 49-51, 78, 80. That is a textbook violation of Section 15(b). *See Rosenbach*, 129 N.E.3d at 1203-04 (holding that a “complaint alleg[ing] that defendants violated the provisions of section 15 of the Act when [they] collected [the plaintiff’s] son’s thumbprint without first following the statutorily prescribed protocol” stated a Section 15(b) claim).

Kronos argues that because “BIPA’s definition of ‘written release’ ... expressly delegates notice and consent obligations *to the employer* when biometric data is collected in the employment context,” it cannot be held liable under Section 15(b). Doc. 62 at 7 (emphasis added). This argument fails to persuade. As an initial matter, even putting aside whether Kronos was required to receive from Plaintiffs the written release mandated by Section 15(b)(3), Kronos still (allegedly) violated Sections 15(b)(1) and (b)(2) by not informing them that it was collecting or obtaining their biometric data, for what purposes, and for how long.

In any event, the statutory definition of “written release” did not relieve Kronos of a Section 15(b)(3) obligation to receive from Plaintiffs a written release before obtaining their data. BIPA defines “written release” as “informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.” 740 ILCS 14/10. Even if Kronos’s obtaining Plaintiffs’ data occurred “in the context of employment”—as opposed to in the context of a business-to-business relationship between Kronos and their employers—Kronos still was a “private entity” that “collect[ed]” or “obtain[ed]” Plaintiffs’ data, and thus remained obligated to receive a release from them as a condition of their employment. Contrary to its submission, imposing that obligation on Kronos would not “be an absurd reading of BIPA.” Doc. 30 at 15. Kronos could have complied by, for example, requiring Plaintiffs’

employers, as a contractual precondition of using a Kronos biometric timekeeping device, to agree to obtain their employees' written consent to Kronos obtaining their data.

Kronos next argues that it did not "collect" Plaintiffs' biometric data within the meaning of Section 15(b) because the provision "applies narrowly only to those entities that actively collect or capture biometrics." *Ibid.* Even if Kronos did not "actively collect" Plaintiffs' data, Section 15(b) governs not only entities that "collect" biometric data, but also those that "capture, purchase, receive through trade, *or* otherwise obtain" such data. 740 ILCS 14/15(b) (emphasis added). The complaint alleges that Kronos "stored," "used," and "disclosed" Plaintiffs' biometric data, Doc. 1-1 at ¶¶ 36, 50, 78, and to have done those things Kronos necessarily first had to "obtain" the data.

Kronos retorts that this result would render Section 15(a) superfluous because, on this understanding of the term "otherwise obtain" in Section 15(b), any entity in "possession" of biometric data for purposes of Section 15(a) would have "otherwise obtain[ed]" such data for purposes of Section 15(b). Doc. 62 at 12. This argument is unpersuasive. Section 15(a) extends to entities that, prior to BIPA's effective date, already possessed biometric information, while Section 15(b) covers only those entities that came into possession of such information after BIPA's effective date. *Compare* 740 ILCS 14/15(a) (covering "[a] private entity *in possession of* biometric identifiers or biometric information") (emphasis added), *with* 740 ILCS 14/15(b) ("No private entity *may* collect, capture, purchase, ... or otherwise obtain a person's ... biometric identifier or biometric information ...") (emphasis added); *see* 740 ILCS 14/99 ("This Act takes effect upon becoming law."). And Section 15(a) imposes different obligations than Section 15(b)—Section 15(a) requires entities to develop and publish written policies regardless of whether they obtained biometric data before or after BIPA's effective date, while

Section 15(b) sensibly imposes notice and consent obligations only on those entities that come into possession of such data after BIPA's effective date. Interpreting the term "obtain" in Section 15(b) to include Kronos's conduct therefore does not render Section 15(a) superfluous.

Not that it matters, *see Al Haj v Pfizer Inc.*, 338 F. Supp. 3d 815 (N.D. Ill. 2018) (holding, against the then-consensus in this District, that *Bristol-Myers Squibb Co. v. Superior Court*, 137 S. Ct. 1773 (2017), does not bar multistate class actions in forums where the defendant is not subject to general jurisdiction), but Kronos is wrong that this result would be an outlier in this District. Specifically, Kronos contends that *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279 (N.D. Ill. 2019), "adds to a unanimous consensus[ that] time clock providers owe no section 15(b) duties when employers use time clocks in the workplace." Doc. 107 at 1. In fact, *Namuwonge* specifically declined to pass on that question because the plaintiff alleged only that her employer had "collected [her] fingerprints using a system that Kronos supplied" and not that "Kronos collected, captured, or otherwise obtained [her] biometric information." *Namuwonge*, 418 F. Supp. 3d at 286 ("[T]he Court does not address the parties' arguments regarding whether section 15(b) requires a private entity other than an employer to secure an executed written release.")). Here, by contrast, Plaintiffs allege that Kronos obtained and stored their biometric data. As to other decisions in this District, they are split on the question whether BIPA governs outside vendors like Kronos in the employment context. *Compare Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088, 1092 (N.D. Ill. 2019) ("To the extent [other] decisions stand for the proposition that the BIPA exempts a third-party non-employer collector of biometric information when an action arises in the employment context, the Court disagrees with those decisions because there is no textual support whatsoever for such a restricted view of the statute's application."), *with Heard v. Becton, Dickinson & Co.*, \_\_ F. Supp. 3d \_\_, 2020 WL

887460, at \*4-5 (N.D. Ill. Feb. 24, 2020) (holding that the plaintiff's allegation that an outside vendor "systematically and automatically collected" his biometric data in connection with his employment did not qualify as the "active" collection required for Section 15(b) liability). The state of the law is by no means "unanimous," and this court is persuaded that the understanding of Section 15(b) set forth above comports with the ordinary meaning of the word "obtain" and does not erase the distinction between Sections 15(a) and 15(b).

**B. Section 15(d) Claim**

Section 15(d) of BIPA provides:

No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

- (1) the subject of the biometric identifier or biometric information ... consents to the disclosure or redisclosure;
- (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject ... ;
- (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
- (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d). The complaint alleges that Kronos disseminated Plaintiffs' biometric data to other firms that hosted the information in their data centers, and it does not suggest that any of the circumstances set forth in subsections (d)(1)-(4) permitted that dissemination. Doc. 1-1 at ¶¶ 45, 79. That is a textbook violation of § 15(d). *See Dixon v. Wash. & Jane Smith Comm.-Beverly*, 2018 WL 2445292, at \*11 (N.D. Ill. May 31, 2018) (holding that the plaintiff's allegation that Kronos obtained her biometric data from her employer without her knowledge or consent stated a Section 15(d) claim against both Kronos and the employer).

Kronos argues that it did not “disclose” Plaintiffs’ biometric information within the meaning of Section 15(d) because “‘disclose’ means ‘to make known or public,’ or ‘to show after a period of inaccessibility or of being unknown.’” Doc. 30 at 13 (quoting *Disclose*, Black’s Law Dictionary (11th ed. 2019)). That argument is beside the point because, as Plaintiffs observe, Doc. 50 at 18 n.4, Section 15(d) covers not just the “disclos[ure]” of biometric data, but also its “disseminat[ion],” and Kronos is alleged to have disseminated their data. Doc. 1-1 at ¶ 45 (“Defendant improperly disseminated [Figueroa’s] biometric identifiers and/or biometric information to third parties, including but not limited to third parties that hosted the biometric data in their data centers ...”), ¶ 79 (“Upon information and belief, Defendant systematically disclosed Plaintiffs’ biometric identifiers and biometric information to other currently unknown third parties, which hosted the biometric data in their data centers.”). It therefore does not matter whether Kronos “disclosed” the data as Kronos understands the term.

Kronos also suggests that Section 15(e) permitted whatever dissemination of Plaintiff’s biometric data it might have conducted. Doc. 30 at 14. Section 15(e) provides in relevant part that a “private entity in possession of a biometric identifier or biometric information shall ... transmit ... biometric information using the reasonable standard of care within the private entity’s industry[] and ... in a manner that is the same as or more protective than the manner in which the private entity ... transmits ... other confidential and sensitive information.” 740 ILCS 14/15(e). Contrary to Kronos’s understanding, Section 15(e) does not affirmatively authorize the dissemination of biometric data outside the four circumstances set forth in subsections (d)(1)-(4); rather, Section 15(e) only sets forth the means by which an entity must transmit biometric data when such transmission is otherwise allowed. *See Namuwonge*, 418 F. Supp. 3d at 285

(“Section 15(d) limits transfers of biometric information while section 15(e) requires that private entities protect biometric information from disclosure.”).

### **C. State of Mind**

Kronos argues that Plaintiffs’ claims should be dismissed because the complaint does not plead any of the mental states required for statutory damages under BIPA. Doc. 30 at 19-20. Section 20 provides that a prevailing plaintiff may recover, “for each violation,” “liquidated damages of \$1,000 or actual damages, whichever is greater,” for negligent violations, and “liquidated damages of \$5,000 or actual damages, whichever is greater,” for reckless or intentional violations. 740 ILCS 14/20(1)-(2). While BIPA subjects defendants to a damage remedy only if there is negligence, recklessness, or willfulness, the cases have split as to whether a defendant’s mental state is a pleading requirement. *Compare Namuwonge*, 418 F. Supp. 3d at 286 (dismissing a BIPA “claim for damages based on intentional and reckless conduct” because the plaintiff did “not allege any substantive details regarding whether the allegations were reckless or intentional”), *with Woodward v. Dylan’s Candybar LLC*, No. 19 CH 05158, slip op. at 7 (Ill. Cir. Nov. 20, 2019) (reproduced at Doc. 101-1 at 8) (“[T]he use of the terms ‘negligent,’ ‘intentional,’ and ‘reckless,’ are standards of culpability for determining damages. The Illinois Supreme Court had made it clear that a plaintiff need not plead facts or elements showing negligence, or reckless or intentional acts in violation of BIPA to be entitled to seek ... liquidated damages ...”).

The court need not choose sides because the complaint adequately alleges negligence on Kronos’s part. “States of mind may be pleaded generally, but a plaintiff still must point to details sufficient to render a claim plausible.” *Pippen v. NBCUniversal Media, LLC*, 734 F.3d 610, 614 (7th Cir. 2013). The complaint alleges that Kronos, as late as 2018 or 2019, continued

to systematically collect and disseminate biometric data without complying with BIPA, which had been enacted a decade earlier in 2008. From that allegation, a plausible inference may be drawn that Kronos acted negligently. *See Namuwonge*, 418 F. Supp. 3d at 286 (“*Namuwonge* has alleged that Kronos failed to maintain a satisfactory biometric data retention policy, despite BIPA taking effect more than ten years ago. The Court ... may plausibly infer from *Namuwonge*’s allegations that Kronos acted negligently.”); *Rogers v. BNSF Ry. Co.*, 2019 WL 5635180, at \*5 (N.D. Ill. Oct. 31, 2019) (“As *Rogers* points out, the BIPA took effect more than ten years ago, and if the allegations of his complaint are true—as the Court must assume at this stage—BNSF has made no effort to comply with its requirements. This is certainly enough, at the pleading stage, to make a claim of negligence or recklessness plausible.”); *Neals*, 419 F. Supp. 3d at 1092-93 (same).

It is unnecessary to decide whether the complaint alleges facts sufficient to raise an inference of recklessness. BIPA provides that recklessness offers a basis for greater liquidated damages, not for a separate claim. 740 ILCS 14/20(2). Because “[a] motion to dismiss under Rule 12(b)(6) doesn’t permit piecemeal dismissals of *parts* of claims,” *BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015), that the complaint’s factual allegations give rise to an inference of negligence is enough to withstand dismissal.

#### **D. Risk of Duplicative Recovery**

In its response to Plaintiffs’ third motion for leave to cite supplemental authority, Kronos raises a new argument as to why payroll vendors like Kronos are not subject to BIPA liability: the risk of the plaintiff obtaining a double recovery from both her employer and the vendor. Doc. 115 at 4-6. Kronos forfeited the argument by waiting until after briefing had closed to raise it. *See Narducci v. Moore*, 572 F.3d 313, 324 (7th Cir. 2009) (“[T]he district court is entitled to find that an argument raised for the first time in a reply brief is forfeited.”);



*Holloman, Sibert, Inc. v. AB Volvo*, 349 F.3d 376, 389 (7th Cir. 2003) (“Because Volvo raised the applicability of the Maine statute in its reply brief, the district court was entitled to find that Volvo waived the issue.”); *Rand v. U.S.*, 2012 WL 1357677, at \*3 n.1 (N.D. Ill. Apr. 18, 2012) (“[T]he court will not address arguments made for the first time in a reply brief or in supplemental filings.”) (citation omitted).

Granted, Kronos did offer—prematurely, as explained below—the risk of duplicative, employer-specific litigation naming Kronos as an additional defendant as a basis for striking the complaint’s *class allegations*. But that is a distinct argument from the one Kronos advances in its supplemental response for dismissing Plaintiffs’ *claims*. And that new argument is without merit in any event, as Plaintiffs’ allegations that Kronos *itself* obtained and disseminated their biometric information reflect a course of conduct distinct from any BIPA violations in which their employers may have engaged, even if such violations occurred simultaneously or through use of the same equipment. *See Dixon*, 2018 WL 2445292, at \*11 (holding that the plaintiff’s allegation that Kronos obtained her biometric data from her employer without her knowledge or consent stated separate BIPA claims against Kronos and her employer).

### **III. Kronos’s Motion to Strike Class Allegations**

Rule 23(c)(1)(A) provides: “At an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action.” Fed. R. Civ. P. 23(c)(1)(A). Although “[m]ost often it will not be ‘practicable’ for the court to do that at the pleading stage, ... sometimes the complaint will make it clear that class certification is inappropriate.” *Hill v. Wells Fargo Bank, N.A.*, 946 F. Supp. 2d 817, 829 (N.D. Ill. 2013) (citing *Gen. Tel. Co. of the Sw. v. Falcon*, 457 U.S. 147, 160 (1982)); *see also Kasalo v. Harris & Harris, Ltd.*, 656 F.3d 557, 563 (7th Cir. 2011) (“Consistent with [Rule 23(c)(1)(A)]’s language, a court may deny class certification even before the plaintiff files a

motion requesting certification.”). That said, “[i]f ... the dispute concerning class certification is factual in nature and discovery is needed to determine whether a class should be certified, a motion to strike the class allegations at the pleading stage is premature.” *Buonomo v. Optimum Outcomes, Inc.*, 301 F.R.D. 292, 295 (N.D. Ill. 2014) (internal quotation marks omitted); *see also Mauer v. Am. Intercont’l Univ., Inc.*, 2016 WL 4698665, at \*2 (N.D. Ill. Sept. 8, 2016) (same). Only if the class allegations are “facially and inherently deficient” should a motion to strike be granted. *Buonomo*, 301 F.R.D. at 295.

Kronos challenges the complaint’s class allegations on superiority, predominance, and adequacy grounds. Those challenges are unpersuasive.

#### **A. Superiority**

Rule 23(b)(3) provides that a class action may be maintained if Rule 23(a) is satisfied and “the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.” Fed. R. Civ. P. 23(b)(3). Factors pertinent to superiority include: “(A) the class members’ interests in individually controlling the prosecution or defense of separate actions; (B) the extent and nature of any litigation concerning the controversy already begun by or against class members; (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (D) the likely difficulties in managing a class action.” *Ibid.* As the Seventh Circuit has explained, the class action device is a superior means of resolving disputes where, as here, any individual class member’s recovery is likely to be small. *See Suchanek v. Sturm Foods, Inc.*, 764 F.3d 750, 759 (7th Cir. 2014) (“The policy at the very core of the class action mechanism is to

overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action prosecuting his or her rights.”) (internal quotation mark omitted).

Observing that the putative class includes some persons pursuing separate lawsuits against their employers in which Kronos is either a defendant or a respondent in discovery, Kronos argues that those other actions are superior venues for litigating the putative class claims brought here. Doc. 33 at 8-9. Insofar as some putative class members have sued Kronos in other suits brought against their respective employers, those persons may be excluded from any certified class if they continue to maintain those suits. *See Bietsch v. Sergeant’s Pet Care Prods., Inc.*, 2016 WL 1011512, at \*12 (N.D. Ill. Mar. 15, 2016) (“Although the class definition may need additional refinement as discovery progresses, the Court will not strike the class allegations at this stage, where it adequately provides [the defendant] with notice of the class Plaintiffs will seek to certify, is definite, and is based on objective criteria. Plaintiffs may further modify the proposed class definition, or the Court may do so on its own initiative, at the class certification stage.”); *Everett v. Baldwin*, 2016 WL 8711476, at \*3 (N.D. Ill. Jan. 15, 2016) (“[W]hen discovery is needed—as it often is—before deciding whether ... a class definition can be modified, courts may deny the motion to strike.”). And the fact that Kronos is a respondent in discovery in suits brought by other putative class members does not bear on superiority, as Kronos cannot avoid class litigation for its own alleged BIPA violations merely because it has information relevant to suits against other defendants.

Kronos also contends that manageability concerns caused by the risk of “duplicative third-party discovery” and the need to monitor simultaneous suits counsel in favor of striking the class claims here. Doc. 33 at 10-12. It is hard to understand how the need to monitor other suits bears on the manageability of class litigation here. Kronos and its able counsel undoubtedly

have the bandwidth to defend this suit as a putative class action while, at the same time, monitoring other BIPA suits in which it is a defendant or a respondent in discovery.

## **B. Predominance**

“Analysis of predominance under Rule 23(b)(3) ‘begins ... with the elements of the underlying cause of action.’” *Messner v. Northshore Univ. HealthSystem*, 669 F.3d 802, 815 (7th Cir. 2012) (quoting *Erica P. John Fund, Inc. v. Halliburton Co.*, 563 U.S. 804, 809 (2011)).

“The Rule 23(b)(3) predominance inquiry tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation.” *Amchem Prods. Inc. v. Windsor*, 521 U.S. 591, 623 (1997). As Justice Ginsburg explained:

To gain class-action certification under Rule 23(b)(3), the named plaintiff must demonstrate, and the District Court must find, that the questions of law or fact common to class members predominate over any questions affecting only individual members. This predominance requirement is meant to test whether proposed classes are sufficiently cohesive to warrant adjudication by representation, but it scarcely demands commonality as to all questions. In particular, when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.

*Comcast Corp. v. Behrend*, 569 U.S. 27, 41 (2013) (Ginsburg, J, dissenting) (alterations, citations, and internal quotation marks omitted); see *Chi. Teachers Union, Local No. 1 v. Bd. of Educ. of City of Chi.*, 797 F.3d 426, 443-44 (7th Cir. 2015) (endorsing Justice Ginsburg’s characterization of the predominance inquiry).

While similar to Rule 23(a)(2) commonality, the predominance requirement is “far more demanding.” *Amchem Prods.*, 521 U.S. at 624. Predominance is not satisfied where liability determinations are individual and fact-intensive, see *Kartman v. State Farm Mut. Auto. Ins. Co.*, 634 F.3d 883, 891 (7th Cir. 2011), and “[m]ere assertion by class counsel that common issues predominate is not enough,” *Parko v. Shell Oil Co.*, 739 F.3d 1083, 1085 (7th Cir. 2014) (alterations omitted). Predominance fails where “affirmative defenses will require a person-by-

person evaluation of conduct to determine whether [a defense] precludes individual recovery.” *Clark v. Experian Info., Inc.*, 233 F.R.D. 508, 512 (N.D. Ill. 2005), *aff’d*, 256 F. App’x 818 (7th Cir. 2007); *see also Myers v. Hertz Corp.*, 624 F.3d 537, 551 (2d Cir. 2010) (“[W]hile it is well established that the existence of a defense potentially implicating different class members differently does not necessarily defeat class certification, it is equally well established that courts must consider potential defenses in assessing the predominance requirement.”) (alterations and citations omitted).

To justify striking class allegations on predominance grounds at the pleadings stage, a defendant must “present ... specific evidence—as opposed to mere speculation—that [a] purportedly individualized issue predominates over common issues.” *Buonomo*, 301 F.R.D. at 298. Kronos argues that the following individualized questions of fact concerning the various timekeeping practices of the putative class members’ myriad employers necessarily defeat predominance: “(i) where, when, and for which employees each employer used Kronos devices; (ii) whether the employer’s compliance with BIPA extends to Kronos; (iii) whether each employee knew and understood that the devices were scanning their fingers; (iv) whether each employer allowed some or all of its employees to opt for other authentication methods ... ; (v) when each employer used Kronos devices, and whether other devices also [sic] in use; and (vi) where each employer stored employee data, for how long, and with what security safeguards.” Doc. 33 at 13-14. Those potential fact questions do not warrant striking the class allegations at the pleading stage. As an initial matter, Kronos fails to explain how those questions bear on its potential liability under BIPA, thereby forfeiting any argument that they justify striking the class allegations. *See G & S Holdings LLC v. Cont’l Cas. Co.*, 697 F.3d 534, 538 (7th Cir. 2012) (“We have repeatedly held that a party waives an argument by failing to make it before the

district court. That is true whether it is an affirmative argument in support of a motion to dismiss or an argument establishing that dismissal is inappropriate.”) (citations omitted).

Even putting aside forfeiture, and as Plaintiffs correctly note, Doc. 51 at 17, the complaint’s allegations give rise to the plausible inference that Kronos knows what biometric data it collected on which employees and for which employers. Doc. 1-1 at ¶¶ 36, 50, 78 (alleging that Kronos systematically collected and stored Plaintiffs’ biometric data in its databases). Whether some employees knew that their employers’ timekeeping devices were scanning their fingerprints, or whether some employees voluntarily opted to use Kronos equipment rather than some other timekeeping method, appears at this point to have no bearing on whether Kronos informed such employees that *it* was collecting their biometric data or whether it obtained their consent. Likewise, the fact that an employer used a different timekeeping method at some other point would have no bearing on Kronos’s liability (or non-liability) for its data collection while the employer used Kronos equipment. And how *employers* stored employee data sheds no light on the relevant question here—how *Kronos* collected and stored such data.

Moreover, even if they were pertinent, the questions raised by Kronos are precisely the sort of fact-intensive issues that generally do not justify striking class allegations at the pleading stage. *See Murdock-Alexander v. Tempsnow Emp’t & Placement Servs., LLC*, 2016 WL 6833961, at \*5 (N.D. Ill. Nov. 21, 2016) (“[W]hen a court considers predominance, it may have to venture into the territory of a claim’s merits and evaluate the nature of the evidence. In most cases, some level of discovery is essential to such an evaluation.”) (internal quotation marks omitted). At most, those questions would counsel in favor of narrowing the class definition at the class certification stage, once discovery sheds light on whether any putative class members

are affected by those questions. *See Messner*, 669 F.3d at 825 (“Defining a class so as to avoid ... being over-inclusive ... is more of an art than a science ... [and] can and often should be solved by refining the class definition rather than by flatly denying class certification on that basis.”); *Smith v. State Farm Mut. Auto. Ins. Co.*, 2015 WL 13658072, at \*3 (N.D. Ill. Jan. 13, 2015) (“[T]he Court agrees with Plaintiffs that it would be premature to strike the class allegations before Plaintiffs have had the opportunity to conduct further discovery, and if necessary, refine their class definition.”).

Kronos maintains that some putative class members may have consented in writing to it obtaining their biometric data. Doc. 33 at 14. That is certainly possible, as Plaintiffs acknowledge. Doc. 51 at 17-18. But having presented no evidence as to how many putative class members gave such consent, Kronos offers no basis to conclude that a significant portion of the putative class has no viable claim. *See Messner*, 669 F.3d at 825 (observing that while “a class should not be certified if it apparent that it contains a great many persons who have suffered no injury at the hands of the defendant[,] ... [t]here is no precise measure for ‘a great many’” and the determination “will turn on the facts as they appear from case to case”). It therefore would be improper at the pleading stage to strike the class allegations on that basis. *See Sullivan v. All Web Leads, Inc.*, 2017 WL 2378079, at \*9 (N.D. Ill. June 1, 2017) (holding, in a Telephone Consumer Protection Act case, that “even if [a] class definition conceptually includes ... consumers who gave ... some sort of individualized consent, it would be premature at th[e] pre-discovery stage to determine whether [a] suit can proceed as a class action” in light of that issue).

Kronos also argues that some putative class members’ claims may be barred by federal labor law preemption, Doc. 33 at 15-16; Doc. 67, or arbitration agreements, Doc. 33 at 16-17.

But again, there is no way of knowing at this stage how many putative class members' claims would be impacted by those issues. *See Messner*, 669 F.3d at 825. And it is speculative at this stage for Kronos to suggest that claims involving a non-employer equipment vendor like Kronos will turn on interpreting a collective bargaining agreement to which it was not a party, *see Miller v. Sw. Airlines Co.*, 926 F.3d 898, 903-904 (7th Cir. 2019) (dismissing BIPA claims brought by unionized employees against their employers where evaluating the claims would require "the interpretation or administration of a collective bargaining agreement" and therefore had to "be resolved by an adjustment board under the Railway Labor Act"), or be foreclosed by arbitration agreements to which it was not a party.

Kronos next argues that because some employees work in industries with "a diminished expectation of privacy," it may have a "waiver defense" turning on individualized workplace conditions. Doc. 33 at 17. But Kronos cites no authority for the proposition that liability under BIPA turns on this consideration. In any event, it is unclear at this juncture what proportion of the putative class works in industries where employees have a diminished expectation of privacy. *See Messner*, 669 F.3d at 825. The same rationale defeats Kronos's argument, Doc. 33 at 17-18, that the complaint's class allegations should be stricken because some putative class members may be subject to BIPA's "government contractor" exception. *See* 740 ILCS 14/25(e) ("Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government."). Nor can Kronos's cursory invocations of *Colorado River* abstention, Doc. 33 at 18, or a "heightened negligence defense" as to Illinois employers with out-of-state headquarters, *id.* at 18-19, justify striking class allegations at this stage, particularly where Kronos makes no effort in its reply to defend those arguments from Plaintiffs' rejoinders, Doc. 51 at 22-24. *See*



*Skinner & Assocs. Ins. Agency v. Norman-Spencer Agency, Inc.*, 845 F.3d 313, 321 (7th Cir. 2017) (“Perfunctory and undeveloped arguments are waived, as are arguments unsupported by legal authority.”). Likewise, Kronos’s unadorned assertion that Plaintiffs fail Rule 23(a)(2)’s commonality requirement, Doc. 33 at 20, which appears to rest on—if anything—the same grounds as its predominance challenge, is both forfeited and unpersuasive.

### **C. Adequacy**

Rule 23(a)(4) provides that named plaintiffs may only “sue ... as representative parties on behalf of all members if,” among other things, they “will fairly and adequately protect the interests of the class.” Fed. R. Civ. P. 23(a)(4). To qualify as an adequate class representative, a “named plaintiff must be a member of the putative class and have the same interest and injury as other members.” *Beaton v. SpeedyPC Software*, 907 F.3d 1018, 1027 (7th Cir. 2018). A named plaintiff “might be inadequate if,” for example, she “is subject to a substantial defense unique to him,” *id.* at 1027-28, has “serious credibility problems,” *Lacy v. Cook Cnty.*, 897 F.3d 847, 866 (7th Cir. 2011), or has a “conflict of interest between [her] and unnamed members of the class,” *Randall v. Rolls-Royce Corp.*, 637 F.3d 818, 824 (7th Cir. 2011).

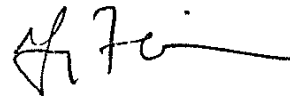
Kronos contends that Figueroa and Burton are inadequate because they will be distracted by litigating the separate BIPA suits they brought against their employers, because they may “sell this putative class short in favor of their employer-specific suits,” and because they will fail to vigorously litigate issues (like labor law preemption) not applicable to them. Doc. 33 at 20. Those challenges cannot be resolved, at least in Kronos’s favor, at the pleading stage. If it turns out that Plaintiffs are not tending properly to this suit or that they are paying insufficient attention to issues that do not directly impact them, the court will have the opportunity to consider those matters at the class certification stage. *See Wilkes v. CareSource Mgmt. Grp. Co.*,

2016 WL 7179298, at \*6 n.2 (N.D. Ind. Dec. 9, 2016) (in resolving a motion to strike class allegations, observing that the defendant's suggestion that "Plaintiffs will be unable to satisfy the ... adequacy requirement[]" was "premature at this stage").

### **Conclusion**

Kronos's motion to dismiss and the motion to strike class allegations are denied. The parties shall file simultaneous briefs by May 5, 2020, addressing whether Plaintiffs have standing to pursue their Section 15(a) claim and, assuming there is no standing, whether that claim should be dismissed for want of jurisdiction or remanded to state court. Kronos shall answer the complaint (other than allegations pertaining only to Section 15(a)) by May 12, 2020.

April 13, 2020



---

United States District Judge